

**Method and Apparatus for Validating a Digital Signature**

Inventor(s) :

Arne Ansper

5 Ahto Buldas

Meelis Roos

Jan Villemson

Abstract of the Disclosure

10 Method and system are described for validating a  
digital signature. More particularly, a signed message  
and a corresponding certificate are received. The  
certificate is checked for validation. A validation  
statement is generated, and the certificate validation and  
15 the signed message provide a status. This status  
represents a request for validation, and is provided along  
with a set of validations among which such status is an  
element. A digest is generated using a Merkle  
authentication tree corresponding to the set of  
20 validations, and this digest is signed with a private key.  
Accordingly, a notary may provide the signed digest,  
status and the set of validations for subsequent  
confirmation of the digital signature.

0973033 03304  
063030 03304